FIPS 140-2 Non-Proprietary Security Policy

for Aruba AP-214, AP-215, AP-224, AP-225, AP-228, AP-274, AP-275, AP-277, AP-324, and AP-325

Wireless Access Points

Version 1.3

February 2020

a Hewlett Packard Enterprise company

www.arubanetworks.com

3333 Scott Blvd
Santa Clara, CA 95054
Phone: 408.227.4500
Fax 408.227.4550

1 Introduction

This document constitutes the non-proprietary Cryptographic Module Security Policy for the Aruba AP-214, AP-215, AP-224, AP-225, AP-228, AP-274, AP-275, AP-277, AP-324, and AP-325 Wireless Access Points with FIPS 140-2 Level 2 validation from Aruba Networks. This security policy describes how the AP meets the security requirements of FIPS 140-2 Level 2, and how to place and maintain the AP in a secure FIPS 140-2 mode. This policy was prepared as part of the FIPS 140-2 Level 2 validation of the product.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Web-site at:

https://csrc.nist.gov/projects/cryptographic-module-validation-program

This document can be freely distributed.

In addition, in this document, the Aruba AP-214, AP-215, AP-224, AP-225, AP-228, AP-274, AP-275, AP-277, AP-324, and AP-325 Wireless Access Points are referred to as the Access Point, the AP, the module, the cryptographic module, and Aruba Wireless AP.

1.1 Acronyms and Abbreviations

AES	Advanced Encryption Standard
AP	Access Point
CBC	Cipher Block Chaining
CLI	Command Line Interface
CO	Crypto Officer
CPSec	Control Plane Security protected
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
ECO	External Crypto Officer
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FE	Fast Ethernet
GE	Gigabit Ethernet
GHz	Gigahertz
HMAC	Hashed Message Authentication Code
Hz	Hertz
IKE	Internet Key Exchange
IPsec	Internet Protocol security
KAT	Known Answer Test
KEK	Key Encryption Key
L2TP	Layer-2 Tunneling Protocol
LAN	Local Area Network
LED	Light Emitting Diode
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SPOE	Serial & Power Over Ethernet
TEL	Tamper-Evident Label
TFTP	Trivial File Transfer Protocol
WLAN	Wireless Local Area Network

2 Product Overview

This section introduces the various Aruba Wireless Access Points, providing a brief overview and summary of the physical features of each model covered by this FIPS 140-2 security policy.

The tested version of the firmware is: **ArubaOS 8.5.0.3-FIPS and ArubaOS 8.2.2.5-FIPS**

Aruba's development processes are such that future releases under AOS 8.2 and 8.5 should be FIPS validate-able and meet the claims made in this document. Only the versions that explicitly appear on the certificate, however, are formally validated. The CMVP makes no claim as to the correct operation of the module or the security strengths of the generated keys when operating under a version that is not listed on the validation certificate.

2.1 AP-214

Figure 1 - Aruba AP-214

This section introduces the Aruba AP-214 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

These compact and cost-effective dual-radio APs deliver wireless data rates of up to 1.3 Gbps to 5-GHz devices with 802.11ac technology. They also support 3×3 MIMO with three spatial streams as well as 2.4-GHz 802.11n clients at data rates up to 450 Mbps. 2.4-GHz (450 Mbps max rate) and 5-GHz (1.3 Gbps max rate) radios, each with 3×3 MIMO and three combined, duplexed (dual-band) external RP-SMA antenna connectors.

When managed by Aruba Mobility Controllers, AP-214 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.1.1 Physical Description

The Aruba AP-214 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic and metal case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through three N-type female connectors for external antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The module hardware version is:

- HW: AP-214-F1 (HPE SKU JW169A)

2.1.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 18 cm (W) x 18c cm (D) x 4.5 cm (H)
- 0.61 kg (1.34 lbs)

2.1.1.2 Interfaces

The module provides the following network interfaces:

- One 10/100/1000BASE-T Ethernet network interface (RJ-45)
- Auto-sensing link speed and MDI/MDX
- 802.3az Energy Efficient Ethernet (EEE)
- USB 2.0 host interface (Type A connector)
- Serial console interface (disabled in FIPS mode by TEL)
- 802.11a/b/g/n/ac Antenna interfaces (External)
- Visual indicators (LEDs):
    - Power/system status
    - Ethernet link status (ENET)
    - Radio status (two; RAD0, RAD1)
- Reset button

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 12V DC power interface

Table 2.1- AP-214 Indicator LEDs

Label	Function	Action	Status
PWR	AP power / ready status	Off	No power to AP
		Red	Initial power-up condition
		Flashing – Green	Device booting, not ready
		On – Green	Device ready
		Orange	AP operating in PoE Power Saving Mode
ENET	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On – Amber	10/100Mbs Ethernet link negotiated

Label	Function	Action	Status
		On – Green	1000Mbps Ethernet link negotiated
		Flashing	Ethernet link activity
2.4GHz	2.4GHz Radio Status	Off	2.4GHz radio disabled
		On – Amber	2.4GHz radio enabled in non-HT WLAN mode
		On – Green	2.4GHz radio enabled in HT WLAN mode
		Flashing – Green	2.4GHz Spectrum or Air Monitor
5GHz	5GHz Radio Status	Off	5GHz radio disabled
		On – Amber	5GHz radio enabled in non-HT WLAN mode
		On – Green	5GHz radio enabled in HT WLAN mode
		Flashing – Green	5GHz Spectrum or Air Monitor

2.2 AP-215

Figure 2 - Aruba AP-215

This section introduces the Aruba AP-215 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

These compact and cost-effective dual-radio APs deliver wireless data rates of up to 1.3 Gbps to 5-GHz devices with 802.11ac technology. They also support 3×3 MIMO with three spatial streams as well as 2.4-GHz 802.11n clients at data rates up to 450 Mbps.

AP-215: Six integrated downtilt omni-directional antennas for 3×3 MIMO with maximum antenna gain of 4.0 dBi in 2.4 GHz and 4.5 dBi in 5 GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. Downtilt angle for maximum gain is roughly 30 degrees.

When managed by Aruba Mobility Controllers, AP-215 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.2.1 Physical Description

The Aruba AP-215 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic and metal case. The module contains 802.11 a/b/g/n/ac transceivers and six internal antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The module hardware version is:

- HW: AP-215-F1 (HPE SKU JW171A)

2.2.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 18 cm (W) x 18 cm (D) x 4.5 cm (H)
- 0.61 kg (1.34 lbs)

2.2.1.2 Interfaces

The module provides the following network interfaces:

- One 10/100/1000BASE-T Ethernet network interface (RJ-45)
- Auto-sensing link speed and MDI/MDX
- 802.3az Energy Efficient Ethernet (EEE)
- USB 2.0 host interface (Type A connector)
- Serial console interface (disabled in FIPS mode by TEL)
- 802.11a/b/g/n/ac Antenna interfaces (Internal) connections
- Visual indicators (LEDs):
    - Power/system status
    - Ethernet link status (ENET)
    - Radio status (two; RAD0, RAD1)
- Reset button

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 12 DC power interface

Table 2.2- AP-215 Indicator LEDs

Label	Function	Action	Status
PWR	AP power / ready status	Off	No power to AP
		Red	Initial power-up condition
		Flashing – Green	Device booting, not ready
		On – Green	Device ready
		Orange	AP operating in PoE Power Saving Mode
ENET	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On – Amber	10/100Mbs Ethernet link negotiated
		On – Green	1000Mbps Ethernet link negotiated
		Flashing	Ethernet link activity
2.4GHz	2.4GHz Radio Status	Off	2.4GHz radio disabled
		On – Amber	2.4GHz radio enabled in non-HT WLAN mode
		On – Green	2.4GHz radio enabled in HT WLAN mode
		Flashing – Green	2.4GHz Spectrum or Air Monitor
5GHz	5GHz Radio Status	Off	5GHz radio disabled
		On – Amber	5GHz radio enabled in non-HT WLAN mode
		On – Green	5GHz radio enabled in HT WLAN mode
		Flashing – Green	5GHz Spectrum or Air Monitor

2.3 AP-224

Figure 3 - Aruba AP-224

This section introduces the Aruba AP-224 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The Aruba AP-224 is high-performance 802.11ac (3x3:3) MIMO, dual-radio (concurrent 802.11a/n/ac + b/g/n/ac) indoor wireless access points capable of delivering combined wireless data rates of up to 1.9 Gbps. These multi-function access points provide wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The access points work in conjunction with Aruba Mobility Controllers to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications

2.3.1 Physical Description

The Aruba AP-224 series Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports three external antennas through 3 X dual-band (RP-SMA) antenna interfaces for supporting external antennas.

The plastic case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- AP-224-F1 (HPE SKU JW173A)
- FIPS Kit
    - 4011570-01 (Part number for Tamper Evident Labels)

2.3.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 20.3 cm (W) x 20.3 cm (D) x 5.4 cm (H).
- 750 g (27 oz)

2.3.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n/ac Antenna (External)
    - 3x RP-SMA antenna interfaces (supports up to 3x3 MIMO with spatial diversity)
- 1 x RJ-45 console interface (disabled in FIPS mode by TEL)
- 1 x USB 2.0

The module provides the following power interfaces:

- 48V DC via Power-over-Ethernet (POE)
- 12V DC power supply

2.3.1.3 Indicator LEDs

There are 5 bicolor (power, ENET and WLAN) LEDs which operate as follows:

Table 2.3- AP-224 Indicator LEDs

Label	Function	Action	Status
PWR	AP power / ready status	Off	No power to AP
		Red	Initial power-up condition
		Flashing – Green	Device booting, not ready
		On – Green	Device ready
		Orange	AP operating in PoE Power Saving Mode
ENET0 ENET1	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On – Amber	10/100Mbs Ethernet link negotiated
		On – Green	1000Mbps Ethernet link negotiated
		Flashing	Ethernet link activity

Label	Function	Action	Status
2.4GHz	2.4GHz Radio Status	Off	2.4GHz radio disabled
		On – Amber	2.4GHz radio enabled in non-HT WLAN mode
		On – Green	2.4GHz radio enabled in HT WLAN mode
		Flashing – Green	2.4GHz Spectrum or Air Monitor
5GHz	5GHz Radio Status	Off	5GHz radio disabled
		On – Amber	5GHz radio enabled in non-HT WLAN mode
		On – Green	5GHz radio enabled in HT WLAN mode
		Flashing – Green	5GHz Spectrum or Air Monitor

2.4 AP-225

This section introduces the Aruba AP-225 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The Aruba AP-225 is high-performance 802.11ac (3x3:3) MIMO, dual-radio (concurrent 802.11a/n/ac + b/g/n/ac) indoor wireless access points capable of delivering combined wireless data rates of up to 1.9 Gbps via three internal antennas. These multi-function access points provide wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The access points work in conjunction with Aruba Mobility Controllers to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications

2.4.1 Physical Description

Figure 4 - Aruba AP-225

The Aruba AP-225 series Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports 3 integrated omni-directional multi-band dipole antenna elements (supporting up to 3x3 MIMO with spatial diversity).

The plastic case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- AP-225-F1 (HPE SKU JW175A)
- FIPS Kit
    - 4011570-01 (Part number for Tamper Evident Labels)

2.4.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 20.3 cm (W) x 20.3 cm (D) x 5.4 cm (H).
- 750 g (27 oz)

2.4.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) ports
- 1 x RJ-45 console interface (Disabled in FIPS mode by TEL)
- 802.11a/b/g/n/ac Antenna Interfaces (Internal)
- 1 x USB 2.0 port

The module provides the following power interfaces:

- 48V DC via Power-over-Ethernet (POE)
- 12V DC power supply

2.4.1.3 Indicator LEDs

There are 5 bicolor (power, ENET and WLAN) LEDs which operate as follows:

Table 2.4 - AP-225 Indicator LEDs

Label	Function	Action	Status
PWR	AP power / ready status	Off	No power to AP
		Red	Initial power-up condition
		Flashing – Green	Device booting, not ready
		On – Green	Device ready
		Orange	AP operating in PoE Power Saving Mode
ENET0 ENET1	Ethernet Network Link Status / Activity	Off	Ethernet link unavailable
		On – Amber	10/100Mbs Ethernet link negotiated
		On – Green	1000Mbps Ethernet link negotiated
		Flashing	Ethernet link activity
2.4GHz	2.4GHz Radio Status	Off	2.4GHz radio disabled
		On – Amber	2.4GHz radio enabled in non-HT WLAN mode
		On – Green	2.4GHz radio enabled in HT WLAN mode
		Flashing – Green	2.4GHz Spectrum or Air Monitor
5GHz	5GHz Radio Status	Off	5GHz radio disabled
		On – Amber	5GHz radio enabled in non-HT WLAN mode
		On – Green	5GHz radio enabled in HT WLAN mode
		Flashing – Green	5GHz Spectrum or Air Monitor

2.5 AP-228

Figure 5 - Aruba AP-228

This section introduces the Aruba AP-228 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The Aruba AP-228 is high-performance 802.11ac (3x3:3) MIMO, dual-radio (concurrent 802.11a/n/ac + b/g/n/ac) indoor wireless access points capable of delivering combined wireless data rates of up to 1.9 Gbps. These multi-function access points provide wireless LAN access, air monitoring, and wireless intrusion detection and prevention over the 2.4-2.5GHz and 5GHz RF spectrum. The access points work in conjunction with Aruba Mobility Controllers to deliver high-speed, secure user-centric network services in education, enterprise, finance, government, healthcare, and retail applications

2.5.1 Physical Description

The Aruba AP-228 series Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through 6 x dual-band (RP-SMA) antenna interfaces for supporting external antennas.

The plastic case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- AP-228-F1 (HPE SKU JW183A)

2.5.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 22.2 cm (L) x 15.0 cm (W) x 7.5 cm (H), 8.5” (L) x 6” (W) x 2.5” (H)
- 1.225 kg/2.700 lbs

2.5.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n/ac Antenna (External)
    - 6x RP-SMA antenna interfaces (supports up to 3x3 MIMO with spatial diversity)
- 1 x micro-USB console interface (disabled in FIPS mode by TEL)

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 110/220V AC power connector

2.5.1.3 Indicator LEDs

Table 2.5 - AP-228 Indicator LED

Label	Action	Status
System LED	Off	No power to AP
	Red	Initial power-up condition
	Flashing – Green	Device booting, not ready
	On – Green	Device ready in 1000Mbps mode. (LED turns off after 1200 seconds)
	Green-Yellow 6 sec.	Device ready in 10/100Mbps mode (LED turns off after 1200 seconds)
	Red	General Fault
	Red – 1 blink off every 3 seconds	Radio 0 fault (5GHz)
	Radio 1 Fault (2.4 GHz)	1000Mbps Ethernet link negotiated

2.6 AP-274

Figure 6 - Aruba AP-274

This section introduces the Aruba AP-274 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The innovative and aesthetically-designed AP-274 outdoor wireless access point delivers gigabit Wi-Fi performance to 802.11ac mobile devices under any weather conditions. Purpose-built to survive in the harshest outdoor environments, AP-274 AP withstands exposure to extreme high and low temperatures, persistent moisture and precipitation, and are fully sealed to keep out airborne contaminants. All electrical interfaces include industrial-strength surge protection. With a maximum data rate of 1.3 Gbps in the 5-GHz band and 600 Mbps in the 2.4-GHz band, AP-274 outdoor AP supports concurrent dual-radio operation at speeds that greatly exceed Fast Ethernet.

When managed by Aruba Mobility Controllers, the AP-274 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.6.1 Physical Description

The Aruba AP-274 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard plastic and metal case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through six N-type female connectors for external antennas.

The metal case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The module hardware version is:

- HW: AP-274-F1 (HPE SKU JW177A)

2.6.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 23 cm (W) x 24 cm (D) x 19 cm (H)
- 2.7 kg (6 lbs)

2.6.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n/ac Antenna (External)
- 1 x micro-USB console interface (disabled in FIPS mode by TEL)

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 110/220V AC power connector

Table 2.6 - AP-274 Indicator LEDs

Label	Action	Status
System LED	Off	No power to AP
	Red	Initial power-up condition
	Flashing – Green	Device booting, not ready
	On – Green	Device ready in 1000Mbps mode. (LED turns off after 1200 seconds)
	Green-Yellow 6 sec.	Device ready in 10/100Mbps mode (LED turns off after 1200 seconds)
	Red	General Fault
	Red – 1 blink off every 3 seconds	Radio 0 fault (5GHz)
	Radio 1 Fault (2.4 GHz)	1000Mbps Ethernet link negotiated

2.7 AP-275

Figure 7 - Aruba AP-275

This section introduces the Aruba AP-275 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The innovative and aesthetically-designed AP-275 outdoor wireless access point delivers gigabit Wi-Fi performance to 802.11ac mobile devices under any weather conditions. Purpose-built to survive in the harshest outdoor environments, AP-275 AP withstands exposure to extreme high and low temperatures, persistent moisture and precipitation, and are fully sealed to keep out airborne contaminants. All electrical interfaces include industrial-strength surge protection. With a maximum data rate of 1.3 Gbps in the 5-GHz band and 600 Mbps in the 2.4-GHz band, AP-275 outdoor AP supports concurrent dual-radio operation at speeds that greatly exceed Fast Ethernet.

When managed by Aruba Mobility Controllers, the AP-275 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.7.1 Physical Description

The Aruba AP-275 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a metal and plastic case. The module contains 802.11 a/b/g/n/ac transceivers and three internal antennas.

The metal case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The module hardware version is:

- HW: AP-275-F1 (HPE SKU JW179A)

2.7.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 23 cm (W) x 24 cm (D) x 27 cm (H)
- 2.4 kg (5.3 lbs)

2.7.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n/ac Antenna Interfaces (Internal)
- 1 x micro-USB console interface (disabled in FIPS mode by TEL)

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 110/220V AC power connector

Table 2.7 - AP-275 Indicator LEDs

Label	Action	Status
System LED	Off	No power to AP
	Red	Initial power-up condition
	Flashing – Green	Device booting, not ready
	On – Green	Device ready in 1000Mbps mode. (LED turns off after 1200 seconds)
	Green-Yellow 6 sec.	Device ready in 10/100Mbps mode (LED turns off after 1200 seconds)
	Red	General Fault

Label	Action	Status
	Red – 1 blink off every 3 seconds	Radio 0 fault (5GHz)
	Radio 1 Fault (2.4 GHz)	1000Mbps Ethernet link negotiated

2.8 AP-277

Figure 8 - Aruba AP-277

This section introduces the Aruba AP-277 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

The innovative and aesthetically-designed AP-277outdoor wireless access points delivers gigabit Wi-Fi performance to 802.11ac mobile devices under any weather conditions. Purpose-built to survive in the harshest outdoor environments, AP-277 AP withstands exposure to extreme high and low temperatures, persistent moisture and precipitation, and are fully sealed to keep out airborne contaminants. All electrical interfaces include industrial-strength surge protection. With a maximum data rate of 1.3 Gbps in the 5-GHz band and 600 Mbps in the 2.4-GHz band, AP-277outdoor AP supports concurrent dual-radio operation at speeds that greatly exceed Fast Ethernet.

When managed by Aruba Mobility Controllers, AP-277 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.8.1 Physical Description

The Aruba AP-277 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a metal and plastic case. The module contains 802.11 a/b/g/n/ac transceivers and three internal antennas.

The metal case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The module hardware version is:

- HW: AP-277-F1 (HPE SKU JW181A)

2.8.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- 23 cm (W) x 24 cm (D) x 27 cm (H)
- 2.0 kg (4.4 lbs)

2.8.1.2 Interfaces

The module provides the following network interfaces:

- 2 x 10/100/1000 Base-T Ethernet (RJ45) Ports
- 802.11a/b/g/n/ac Antenna Interfaces (three Internal)
- 1 x micro-USB console interface (disabled in FIPS mode by TEL)

The module provides the following power interfaces:

- Power-over-Ethernet (POE)
- 110/220V AC power connector

Table 2.8 - AP-277 Indicator LED

Label	Action	Status
System LED	Off	No power to AP
	Red	Initial power-up condition
	Flashing – Green	Device booting, not ready
	On – Green	Device ready in 1000Mbps mode. (LED turns off after 1200 seconds)
	Green-Yellow 6 sec.	Device ready in 10/100Mbps mode (LED turns off after 1200 seconds)
	Red	General Fault
	Red – 1 blink off every 3 seconds	Radio 0 fault (5GHz)
	Radio 1 Fault (2.4 GHz)	1000Mbps Ethernet link negotiated

2.9 AP-324

Figure 9 - Aruba AP-324

This section introduces the Aruba AP-324 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

With a maximum concurrent data rate of 1,733 Mbps in the 5 GHz band and 600 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.3Gbps), the 320 Series Access Points deliver a best-in-class, next-generation 802.11ac Wi-Fi infrastructure that is ideal for lecture halls, auditoriums, public venues, and high-density office environments. Four RP-SMA connectors provide connections for dual band antennas.

When managed by Aruba Mobility Controllers, AP-324 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.9.1 Physical Description

The Aruba AP-324 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through four N-type female connectors for external antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: AP-324-F1 (HPE SKU JW185A)

2.9.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (unit, excluding mount accessories): 203mm (W) x 203mm (D) x 57mm (H) 8.0” (W) x 8.0” (D) x 2.2” (H) - 950g/34oz
- Dimensions/weight (shipping): 315mm (W) x 265mm (D) x 100mm (H) 12.4” (W) x 10.4” (D) x 3.9” (H) - 1350g/48oz

Environmental

- Operating: - Temperature: 0° C to +50° C (+32° F to +122° F) - Humidity: 5% to 95% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

2.9.1.2 Interfaces

The module provides the following network interfaces:

- Two 10/100/1000BASE-T Ethernet network interfaces (RJ-45)
- Auto-sensing link speed and MDI/MDX
- Link Aggregation support to achieve platform throughput up to 2 Gbps
- 802.3az Energy Efficient Ethernet (EEE)
- PoE-PD: 48 Vdc (nominal) 802.3af or 802.3at PoE

DC power interface, 48Vdc nominal, +/- 5%

- 1.35/3.5-mm center-positive circular plug with 9.5-mm length

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio

- Up to 4dBm transmit power (class 2) and -91dBm receive sensitivity

Other Interfaces

- Visual indicators (tri-color LEDs): For system and radio status
- Reset button: Factory reset (during device power up)
- Serial console interface (proprietary; optional adapter cable available; disabled in FIPS mode)

Table 2.9: AP-324 LED Status Indicators

System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green- Solid	Device ready
	Amber- Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition
Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green- Solid	Both radios enabled in access mode

	Amber- Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	One radio enabled in access mode, one enabled in monitor mode

2.10 AP-325

Figure 10 - Aruba AP-325

This section introduces the Aruba AP-325 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

With a maximum concurrent data rate of 1,733 Mbps in the 5 GHz band and 600 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.3Gbps), the 320 Series Access Points deliver a best-in-class, next-generation 802.11ac Wi-Fi infrastructure. The high performance and high density 802.11ac 320 Series Access Points support dual radio 4x4 802.11AC multi-user MIMO with 4SS/VHT80 5GHz and 4SS/HT40 2.4GHz.

When managed by Aruba Mobility Controllers, AP-325 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.10.1 Physical Description

The Aruba AP-325 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and leveraging eight integrated omni-directional downtilt antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: AP-325-F1 (HPE SKU JW187A)

2.10.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (unit, excluding mount accessories): 203mm (W) x 203mm (D) x 57mm (H) 8.0” (W) x 8.0” (D) x 2.2” (H) - 950g/34oz
- Dimensions/weight (shipping): 315mm (W) x 265mm (D) x 100mm (H) 12.4” (W) x 10.4” (D) x 3.9” (H) - 1350g/48oz

Environmental

- Operating: - Temperature: 0° C to +50° C (+32° F to +122° F) - Humidity: 5% to 95% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

2.10.1.2 Interfaces

The module provides the following network interfaces:

- Two 10/100/1000BASE-T Ethernet network interfaces (RJ-45)
- Auto-sensing link speed and MDI/MDX
- Link Aggregation support to achieve platform throughput up to 2 Gbps
- 802.3az Energy Efficient Ethernet (EEE)
- PoE-PD: 48 Vdc (nominal) 802.3af or 802.3at PoE

DC power interface, 48Vdc nominal, +/- 5%

- 1.35/3.5-mm center-positive circular plug with 9.5-mm length

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio

- Up to 4dBm transmit power (class 2) and -91dBm receive sensitivity

Other Interfaces

- Visual indicators (tri-color LEDs): For system and radio status
- Reset button: Factory reset (during device power up)
- Serial console interface (proprietary; optional adapter cable available; disabled in FIPS mode)

Table 2.10: AP-325 LED Status Indicators

System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green- Solid	Device ready
	Amber- Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Restricted mode: * Uplink negotiated in sub optimal speed; or

		* Radio in non-high throughput (HT) mode
	Red	System error condition
Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green- Solid	Both radios enabled in access mode
	Amber- Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	One radio enabled in access mode, one enabled in monitor mode

3 Module Objectives

This section describes the assurance levels for each of the areas described in the FIPS 140-2 Standard. .

3.1 Security Levels

Table 3.1 - Security Levels

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**2**

3.2 Physical Security

The Aruba Wireless AP is a scalable, multi-processor standalone network device and is enclosed in a robust metal and/or plastic housing. The AP enclosure is resistant to probing (please note that this feature has not been validated as part of the FIPS 140-2 validation) and is opaque within the visible spectrum. The enclosure of the AP has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

3.2.1 Applying TELs

The Crypto Officer must apply Tamper-Evident Labels (TELs) to the AP to allow detection of the opening of the device, and to block the serial console port (on the bottom of the device). The TELs shall be installed for the module to operate in a FIPS Approved mode of operation. Vendor provides FIPS 140 designated TELs which have met the physical security testing requirements for tamper evident labels under the FIPS 140-2 Standard. TELs are not endorsed by the Cryptographic Module Validation Program (CMVP). Aruba provides double the required amount of TELs with shipping and additional replacement TELs can be obtained by calling customer support and requesting part number 4011570-01 (HPE SKU JY894A).

The Crypto Officer is responsible for securing and having control at all times of any unused tamper evident labels. If evidence of tampering is found with the TELs, the module must immediately be powered down and the administrator must be made aware of a physical security breach. The Crypto Officer should employ TELs as follows:

- Before applying a TEL, make sure to clean the target surfaces with alcohol and let dry.
- Do not cut, trim, punch, or otherwise alter the TEL.

- Apply the wholly intact TEL firmly and completely to the target surfaces.
- Ensure that TEL placement is not defeated by simultaneous removal of multiple modules.
- Allow 24 hours for the TEL adhesive seal to completely cure.
- Record the position and serial number of each applied TEL in a security log.
- To obtain additional or replacement TELS, please order Aruba Networks part number: 4011570-01.

Once applied, the TELs included with the AP cannot be surreptitiously broken, removed or reapplied without an obvious change in appearance:

Each TEL has a unique serial number to prevent replacement with similar label. To protect the device from tampering, TELs should be applied by the Crypto Officer as pictured below:

3.2.2 TELs Placement

This section displays all the TELs locations on each of module.

3.2.2.1 TELs Placement on the AP-214

The AP-214 requires 3 TELs. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 11 and 12 for placement.

Figure 11 - Top View of AP-214 with TELs

Figure 12 – Bottom View of AP-214 with TELs

3.2.2.2 TEL Placement on the AP-215

The AP-215 requires 3 TELS. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 13 and 14 for placement.

Figure 13 – Top View of AP-215 with TELs

Figure 14 – Bottom View of AP-215 with TELs

3.2.2.3 TEL Placement on the AP-224/225

This section displays all the TEL locations of the Aruba AP-224/225. The AP-224/225 requires a minimum of 4 TELs to be applied as follows:

To detect opening of the chassis cover:

- Spanning the bottom and top chassis covers and placed on the left, right, and bottom of the unit

To detect access to restricted ports

- Spanning the serial port

Following is the TEL placement for the AP-224/225:

Figure 15: AP-224/225 Front/Top view

Figure 16: AP-224/225 Back/Bottom View

3.2.2.4 TEL Placement on the AP-274

The AP-274 requires a minimum of 6 TELS. Two sealing the top plate (labels 1 and 2), see Figure 17. One covering the console port (label 3) and one securing the body to the bottom (label 4), see Figure 18. Finally apply one label to each side sealing it to the bottom (labels 5 & 6), see figures 19 and 20 for placement.

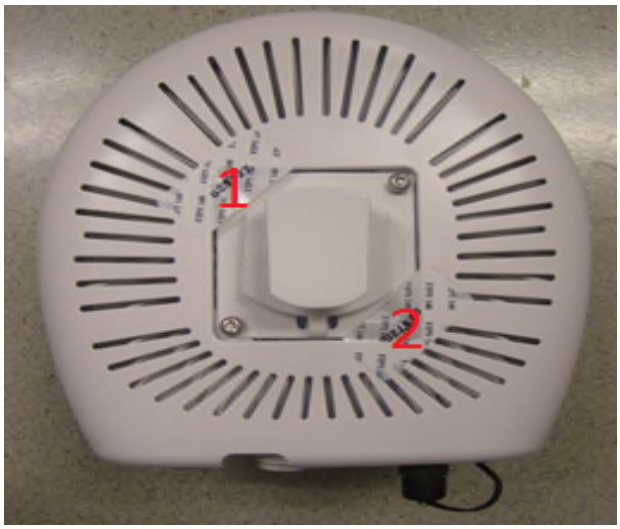

Figure 17 – Top View of AP–274 with TELs

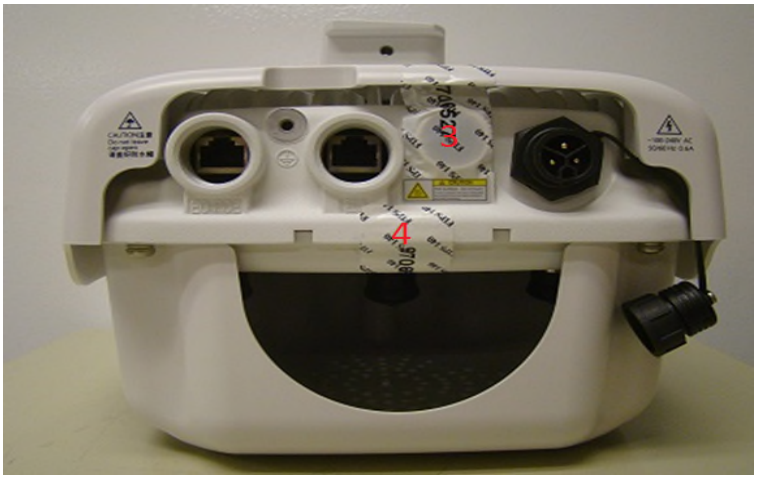

Figure 18 – Rear View of AP-274 with TELs

Figure 19 – Right Side View of AP-274 with TELs

Figure 20 – Left Side View of AP-274 with TELs

3.2.2.5 TEL Placement on the AP-275

The AP-275 requires a minimum of 6 TELS. Two sealing the top plate (labels 1 and 2), see Figure 21. One covering the console port (label 3) and one securing the body to the bottom (label 4), see Figure 22. Finally apply one label to each side sealing it to the bottom (labels 5 & 6), see figures 23 and 24 for placement.

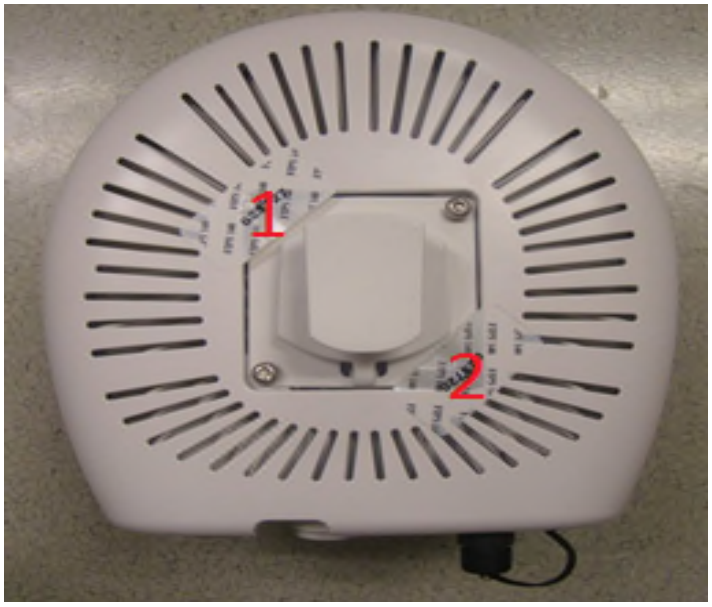

Figure 21 – Top View of AP–275 with TELs

Figure 22 – Rear View of AP-275 with TELs

Figure 23 – Right Side View of AP-275 with TELs

Figure 24 – Left Side View of AP-275 with TELs

3.2.2.6 TEL Placement on the AP-277

The AP-277 requires a minimum of 3 TELS. One covering the console port (label 1) see Figure 25. Apply one label to each side sealing it to the bottom (labels 2 & 3), see figures 26 and 27 for placement.

Figure 25 – Top View of AP–277 with TELs

Figure 26 – Right Side View of AP-277 with TELs

Figure 27 – Left Side View of AP-277 with TELs

3.2.2.7 TEL Placement on the AP-228

This section displays all the TEL locations of the Aruba AP-228. The AP-228 requires a minimum of 3 TELs to be applied as follows:

To detect opening of the chassis cover:

- Spanning the bottom and top chassis covers and placed on the left, right of the unit

To detect access to restricted ports

- Spanning the console port

Figure 28: AP-228 Front/Top view

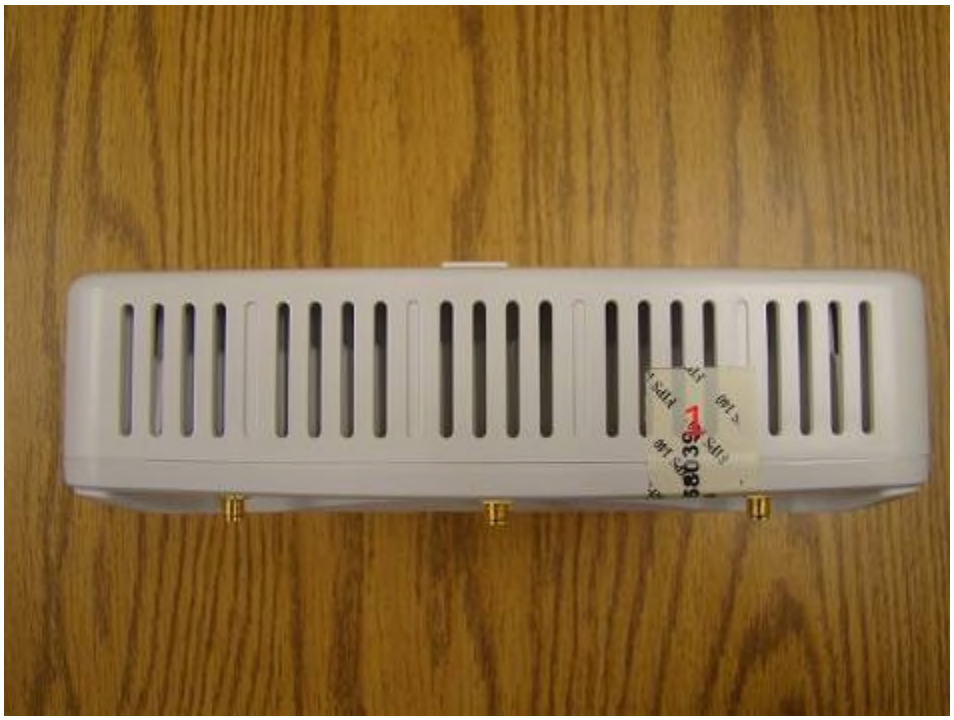

Figure 29: AP-228 Edge View to show TEL wrapping.

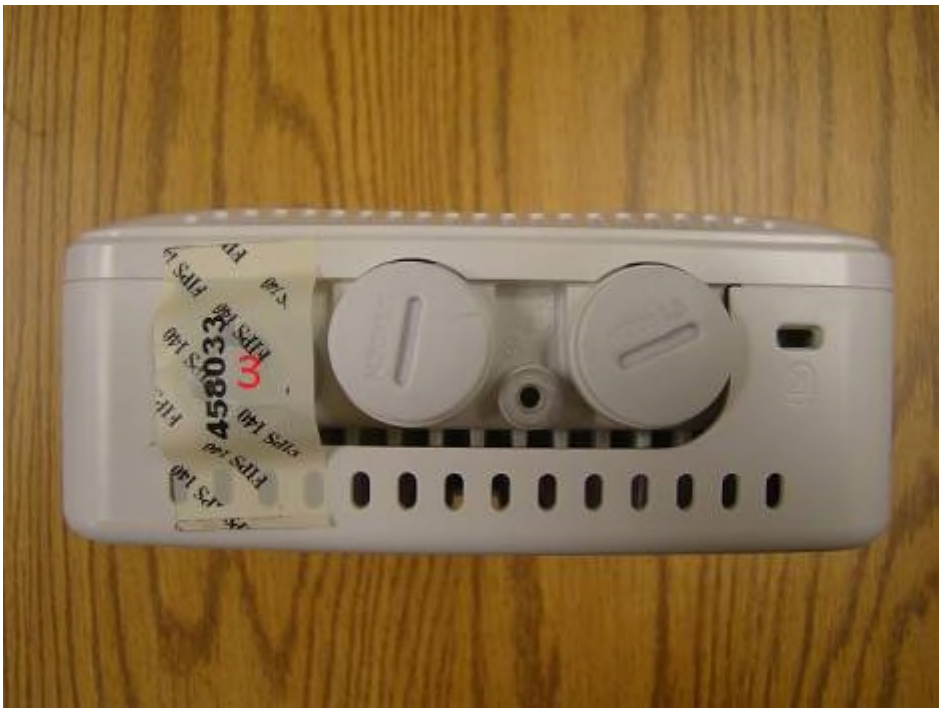

Figure 30: AP-228 End view to show console port coverage

3.2.2.8 TELs Placement on the AP-324

The AP-324 requires three TELs. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 31 and 32 for placement.

Figure 31 - Top View of AP-324 with TELs

Figure 32 – Bottom View of AP-324 with TELs

3.2.2.9 TEL Placement on the AP-325

The AP-325s require 3 TELS. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 33 and 34 for placement.

Figure 33 – Top View of AP-325 with TELs

Figure 34 – Bottom View of AP-325 with TELs

3.2.3 Inspection/Testing of Physical Security Mechanisms

Table 3.2 - Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanism	Recommended Test Frequency	Guidance

Tamper-evident labels (TELs)	Once per month	Examine for any sign of removal, replacement, tearing, etc. See images above for locations of TELs. If any TELS are found to be missing or damaged, contact a system administrator immediately
Opaque module enclosure	Once per month	Examine module enclosure for any evidence of new openings or other access to the module internals. If any TELS are found to be missing or damaged, contact a system administrator immediately

3.3 Operational Environment

The FIPS 140-2 Operational Environment requirements are not applicable because the module is designated as a non-modifiable operational environment. The module only allows the loading of trusted and verified firmware that is signed by Aruba.

3.4 Logical Interfaces

The physical interfaces are divided into logical interfaces defined by FIPS 140-2 as described in the following table.

Table 3.3 - Logical Interfaces

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	• 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces
Data Output Interface	• 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces
Control Input Interface	• 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces • Reset button (AP-214/215)
Status Output Interface	• 10/100/1000 Ethernet Ports • 802.11a/b/g/n/ac Antenna Interfaces
Power Interface	• Power Input • Power-over-Ethernet (POE)

Data input and output, control input, status output, and power interfaces are defined as follows:

- Data input and output are the packets that use the networking functionality of the module.
- Control input consists of manual control inputs for power and reset through the power interfaces (power supply or POE). It also consists of all of the data that is entered into the access point while using the management interfaces. A reset button is present which is used to reset the AP to factory default settings.

- Status output consists of the status indicators displayed through the LEDs, the status data that is output from the module while using the management interfaces, and the log file.
    - LEDs indicate the physical state of the module, such as power-up (or rebooting), utilization level, and activation state. The log file records the results of self-tests, configuration errors, and monitoring data.
- The module may be powered by an external power supply. Operating power may also be provided via Power Over Ethernet (POE) device, when connected, the power is provided through the connected Ethernet cable.
- Console port is disabled when operating in FIPS mode by TEL.

The module distinguishes between different forms of data, control, and status traffic over the network ports by analyzing the packet headers and contents.

4 Roles, Authentication and Services

4.1 Roles

The module supports the role-based authentication of Crypto Officer, User, and Wireless Client; no additional roles (e.g., Maintenance) are supported. Administrative operations carried out by the Aruba Mobility Controller or Aruba Mobility Master map to the Crypto Officer role. The Crypto Officer has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs. Configuration can be performed through a standalone Mobility Controller or by a Mobility Master if deployed in the environment. The Mobility master also acts as a CO for the APs.

Defining characteristics of the roles depend on whether the module is configured as in either Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode or Mesh AP FIPS Mode. There are four FIPS approved modes of operations, which are Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode and the two Mesh Modes, Mesh Portal FIPS Mode and Mesh Point FIPS Mode. Please refer to section 8 in this documentation for more information.

- **Remote AP FIPS mode**:
    - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
    - User role: in the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer role.
    - Wireless Client role: in Remote AP FIPS mode configuration, a wireless client can create a connection to the module using 802.11i and access wireless network access/bridging services. When Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via 802.11i Pre-shared secret only.

- **CPSec Protected AP FIPS mode**:
    - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
    - User role: in the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer
    - Wireless Client role: in CPSec Protected AP FIPS mode configuration, a wireless client can create a connection to the module using 802.11i Pre-shared secret and access wireless network access services.
- **Mesh Portal FIPS mode:**
    - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
    - User role: the adjacent Mesh Point APs in a given mesh cluster. Please notice that Mesh Portal AP must be physically wired to Mobility Controller.
    - Wireless Client role: in Mesh Portal FIPS AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.
- **Mesh Point FIPS mode:**

- Crypto Officer role: the Crypto Officer role is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs. The first mesh AP configured is the only AP with the direct wired connection.
- User role: the adjacent Mesh APs in a given mesh cluster. Please notice that User role can be a Mesh Point AP or a Mesh Portal AP in the given mesh network.
- Wireless Client role: in Mesh Mesh Point FIPS AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.

4.1.1 Crypto Officer Authentication

In each of FIPS approved modes, the Aruba Mobility Controller or Mobility Master implements the Crypto Officer role. Connections between the module and the mobility controller are protected using IPSec. Crypto Officer's authentication is accomplished via either Pre-shared secret (IKEv1), RSA digital certificate (IKEv1/IKEv2) or ECDSA digital certificate (IKEv2). The Mobility Master interacts with the APs through the Mobility Controller through provisioning of configurations.

4.1.2 User Authentication

Authentication for the User role depends on the module configuration. When the module is configured in Mesh Portal FIPS mode or Mesh Point FIPS mode, the User role is authenticated via the WPA2 pre-shared key or EAP. When the module is configured as a Remote AP FIPS mode and CPSec protected AP FIPS mode, the User role is authenticated via the same IKEv1/IKEv2 pre-shared key or RSA/ECDSA certificate that is used by the Crypto Officer.

4.1.3 Wireless Client Authentication

The wireless client role defined in each of FIPS approved modes authenticates to the module via 802.11i. Please notice that WEP and TKIP configurations are not permitted in FIPS mode. When Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via 802.11i Pre-shared secret only.

4.1.4 Strength of Authentication Mechanisms

The following table describes the relative strength of each supported authentication mechanism.

Table 4.1 - Strength of Authentication Mechanisms

Authentication Mechanism	Mechanism Strength

Authentication Mechanism	Mechanism Strength
IKEv1 Pre-shared secret based authentication (CO/User role)	Passwords are required to be a minimum of eight ASCII characters and a maximum of 64 with a minimum of one letter and one number, or the password must be exactly 64 HEX characters. Assuming the weakest option of 8 ASCII characters with the listed restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it's double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/3,608,347,333,959,680, which is less than 1 in 100,000 required by FIPS 140-2.
802.11i Pre-shared secret based authentication (Wireless Client and Mesh AP user roles)	Passwords are required to be a minimum of eight ASCII characters and a maximum of 63 with a minimum of one letter and one number, or the password must be exactly 64 HEX characters. Assuming the weakest option of 8 ASCII characters with the listed restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it's double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/3,608,347,333,959,680, which is less than 1 in 100,000 required by FIPS 140-2.
RSA Certificate based authentication (CO/User role)	The module supports 2048-bit RSA key authentication during IKEv1 and IKEv2. RSA 2048 bit keys correspond to 112 bits of security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^112, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/2^112, which is less than 1 in 100,000 required by FIPS 140-2.
ECDSA Certificate based authentication (CO/User role)	ECDSA signing and verification is used to authenticate to the module during IKEv1/IKEv2. Both P-256 and P-384 curves are supported. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security. Assuming the low end of that range, the associated probability of a successful random attempt during a one-minute period is 1 in 2^128, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is 60,000/2^128, which is less than 1 in 100,000 required by FIPS 140-2.

4.2 Services

The module provides various services depending on role. These are described below.

4.2.1 Crypto Officer Services

The CO role in each of FIPS modes defined in section 4.1 has the same services.

Table 4.2.1 - Crypto Officer Services

Services	**Description**	**CSPs Accessed** (see section 6 below for a complete description to each CSP and the associated cryptographic algorithms)
FIPS mode enable/disable	The CO enables FIPS mode by following the procedures under Section 8 to ensure the AP is configured for Secure Operations. The CO can disable FIPS mode by reverting these changes.	None.
Key Management	The CO can cause the module to generate the SKEYSEED and can configure/modify the IKEv1/IKEv2 shared secret and the 802.11i Pre-shared secret (used in advanced Remote AP configuration). The CO can add/overwrite IKEv1/IKEv2 certificates (the RSA and ECDSA private keys are protected by non-volatile memory and cannot be modified). Also, the CO implicitly uses the KEK to read/write configuration to non-volatile memory.	1, 13, 16, 22, 24, and 25 (read), 13, 16, 22, 24 and 25 (write)
Remotely reboot module	The CO can remotely trigger a reboot	None
Self-test triggered by CO/User reboot	The CO can trigger a programmatic reset leading to self-test and initialization	None
Update module firmware[1]	The CO can trigger a module firmware update	1,12 (read)
Configure non-security related module parameters	CO can configure various operational parameters that do not relate to security	None.

[1] Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Services	**Description**	**CSPs Accessed** (see section 6 below for a complete description to each CSP and the associated cryptographic algorithms)
Creation/use of secure management session between module and CO[2]	The module supports use of IPSec for securing the management channel.	2, 3, 4, 5. 6, 7, .8, 9, 10, 11 (read, write) 12 (read) 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24 (read, write)
System Status	CO may view system status information through the secured management channel	See creation/use of secure management session above.
Creation/use of secure mesh channel[3]	The module requires secure connections between mesh points using 802.11i	1, 25 (read) 26, 27, 28, 29, 30 (read/write)
Zeroization	The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys (IKEv1 Pre-shared key and 802.11i Pre-Shared Key) stored in the flash can be zeroized by using command 'ap wipe out flash' or by overwriting with a new secret. The 'no' command in the CLI can be used to zeroize IKE, Ipsec CSPs. Please See CLI guide for details. The other keys/CSPs (RSA/ECDSA public key/private key and certificate) stored in Flash memory can be zeroized by using command 'ap wipe out flash'.	All CSPs (not including the Factory CA Public Key) will be destroyed.
Openflow Agent	Agent run on device for use with Mobility Master SDN. Leveraged by the SDN for discovering of hosts and networks, configuration of networks, and collection of statistics.	None

4.2.2 User Services

The User role for Remote AP FIPS mode and Control Plane Security (CPSec) Protected AP FIPS mode supports the same services listed in the Section 4.2.1 Crypto Officer Services.

[2] This service is *not* available in Mesh Point FIPS mode. In Mesh Point mode, the IPSec tunnel will be between the Mesh Portal and the controller, not the Mesh Point and the controller.

[3] This service is only applicable in the Mesh Portal FIPS mode and Mesh Point FIPS mode. It is not applicable in Control Plane Security (CPSec) Protected AP FIPS mode and Remote AP FIPS mode.

The User role for Mesh Portal FIPS mode and Mesh Point FIPS mode supports the services listed in Section 4.2.3 Wireless Client Services.

4.2.3 Wireless Client Services

The following module services are provided for the Wireless Client role in Remote AP FIPS mode, CPSec protected AP FIPS mode, Mesh Portal FIPS mode and Mesh Point FIPS mode.

Table 4.2.3- Wireless Client Services

Service	**Description**	**CSPs Accessed** (see section 6 below for a complete description to each CSP and the associated cryptographic algorithms)
Generation and use of 802.11i cryptographic keys	In all modes, the links between the module and wireless client are secured with 802.11i.	1, 25 (read) 26,27,28,29,30 (read/write)
Use of 802.11i Pre-shared secret for establishment of IEEE 802.11i keys	When the module is in advanced Remote AP configuration, the links between the module and the wireless client are secured with 802.11i. This is authenticated with a shared secret only.	1, 25 (read)
Wireless bridging services	The module bridges traffic between the wireless client and the wired network.	None

4.2.4 Unauthenticated Services

The module provides the following unauthenticated services, which are available regardless of role.

- System status – module LEDs
- Reboot module by removing/replacing power
- Self-test and initialization at power-on.

4.2.5 Service Available in Non-FIPS Mode

All of the services that are available in FIPS mode are also available in non-FIPS mode.

• If not operating in the Approved mode as per the procedures in section 8, then non-Approved algorithms and/or sizes are available.

• Upgrading the firmware via the console port.

• Debugging via the console port.

4.2.6 Non-Approved Services Disallowed in FIPS Mode

- The Suite-B (bSec) protocol is a pre-standard protocol that has been proposed to the IEEE 802.11 committee as an alternative to 802.11i.
- WPA3
- WPA-2 Multiple Pre-Shared Key (MPSK), where every client connected to the WLAN SSID may have its own unique PSK.
- IPSec/IKE using Triple-DES

5 Cryptographic Algorithms

The firmware in each module contains the following cryptographic algorithm implementations/crypto libraries to implement the different FIPS approved cryptographic algorithms that will be used for the corresponding security services supported by the module in FIPS mode: NOTE: The modes listed for each algorithm are only those actually used by the module (additional modes may have been tested during CAVS testing and not currently used).

- ArubaOS OpenSSL Module algorithm implementation
- ArubaOS Crypto Module algorithm implementation
- ArubaOS UBOOT Bootloader algorithm implementation
- Aruba AP Hardware algorithm implementation

Below are the detailed lists for the FIPS approved algorithms and the associated certificate implemented by each crypto library

ArubaOS OpenSSL					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2900, 3998	AES	FIPS 197, SP 800-38A	ECB, CBC, CFB (128only), CTR (ext only)	128, 192, 256	Data Encryption/Decryption
825, 2152	CVL RSASP1 PKCS 1.5	FIPS 186-4		MOD 2048	RSA
326, 826	CVL IKEv1	SP 800-135 Rev1	IKEv1(DSA, PSK 2048, SHA-256, 384),	MOD 2048	Key Derivation
528, 1188	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Number Generation
1578, 1580	ECDSA	FIPS 186-2	PKV, SigVer	P256, P384	Digital Key and Signature Verification
1578, 1580	ECDSA	FIPS 186-4	PKG, PKV, SigGen, SigVer	P256, P384	Digital Key Generation and Verification, Signature Generation and Verification
1835, 2610	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
32, 92	KBKDF	SP 800-108	CTR	HMAC-SHA1,HMAC-SHA256, HMAC-	Deriving Keys

				SHA384	
1528, 2054	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048, 1024 (for legacy SigVer only)	Digital Signature Verification
1528, 2054	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Digital Key Generation, Signature Generation and Verification
1500, 1502	DSA	FIPS 186-4		2048	Key Generation, PQG Generation
2440, 3300	SHS	FIPS 180-4	SHA-, SHA-256, SHA-384, SHA-512 Byte Only		Message Digest
1726, 2196	Triple-DES	SP 800-67 Rev2	TEBC, TCBC	192	Data Encryption/Decryption
AES 2900 HMAC 1835	KTS	SP 800-38F	AES-CBC[4]	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec
AES 3998 HMAC 2610	KTS	SP 800-38F	AES-CBC[5]	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec

Note:

- In FIPS Mode, Triple-DES is only used in the Self-Tests and with the KEK.

ArubaOS Crypto Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2884, 4138	AES	FIPS 197, SP 800-38A SP800-38D	CBC, GCM, CTR (ext only)	128, 192, 256	Data Encryption/Decryption
944, 2154	CVL IKEv2	SP800-135 Rev1	IKEv2(2048 SHA-256, 384)		Key Derivation
313, 2156	RSASP1	FIPS	2048 PKCS		Key Gen, SigVer,

[4] key establishment methodology provides between 128 and 256 bits of encryption strength

[5] key establishment methodology provides between 128 and 256 bits of encryption strength

		186-4	#1.5		SigGen
519, 950, 1210, 1211	ECDSA	FIPS 186-2	PKV, SigVer	P256, P384	Digital Key and Signature Verification
519, 950, 1210, 1211	ECDSA	FIPS 186-4	PKG, PKV, SigGen, SigVer	P256, P384	Digital Key Generation and Verification, Signature Generation and Verification
1292, 1293	DSA	FIPS 186-4	PQG, KeyGen	2048	Digital Signature Generation and Verification
1818, 2711	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
1518, 2254	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	1024 (legacy Siger only), 2048	Digital Signature Verification
1518, 2254	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Digital Key Generation, Signature Generation and Verification
2425, 3408	SHS	FIPS 180-4	SHA-1,SHA-256, SHA-384, SHA-512 Byte Only		Message Digest
1720, 2262	Triple-DES	SP 800-67 Rev2	TEBC, TCBC	192	Data Encryption/Decryption
AES 2884	KTS	SP 800-38F	AES-GCM[6]	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec
AES 2884 HMAC 1818	KTS	SP 800-38F	AES-CBC[7]	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec
AES 4138	KTS	SP 800-38F	AES-GCM[8]	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec

[6] key establishment methodology provides between 128 and 256 bits of encryption strength

[7] key establishment methodology provides between 128 and 256 bits of encryption strength)

[8] key establishment methodology provides between 128 and 256 bits of encryption strength

AES 4138 HMAC 2711	KTS	SP 800-38F	AES-CBC[9]	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec

Note:

- In FIPS Mode, Triple-DES is only used in the Self-Tests.
- The algorithms in the table are not used when the module is configured into the Mesh Point FIPS mode

ArubaOS UBOOT Bootloader					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2395, 2419	RSA	FIPS 186-4	SHA-1, SHA-256	2048	Digital Signature Verification
3633, 3657	SHS	FIPS 180-4	SHA-1, Sha-256, Byte Only	160, 256	Message Digest

NOTE: Only Firmware signed with SHA-256 is permitted in the Approved mode. Digital signature verification with SHA-1, while available within the module, shall only be used while in the non-Approved mode.

Aruba AP Hardware					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
1648, 1649, 5412	AES	FIPS 197, SP 800-38A SP800-38C	ECB, CBC, CFB128, OFB, CTR (ext only) CCM, GCM(used for self-test only)	128, 192, 256	Data Encryption/Decryption
538 & 967	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 256, 384, 512	Message Authentication
934 & 1446	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only	160, 256, 384, 512	Message Digest
758 & 1075	Triple-DES	SP 800-67	TEBC, TCBC,	192	Data

[9] key establishment methodology provides between 128 and 256 bits of encryption strength)

		Rev2	TOFB		Encryption/Decryption

Note: In FIPS Mode, Triple-DES is only used in the Self-Tests.

Non-FIPS Approved Algorithms Allowed in FIPS Mode

- NDRNG (used solely to seed the approved DRBG)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)

NOTE: IKEv1 and IKEv2 protocols have not been reviewed or tested by the CAVP and CMVP.

Non-FIPS Approved Cryptographic Algorithms used only in Non-FIPS 140 Mode

The cryptographic module implements the following non-approved algorithms that are not permitted for use, and are not used, in the FIPS 140-2 mode of operations:

- DES
- HMAC-MD5
- MD5
- RC4
- RSA (non-compliant less than 112 bits of encryption strength)
- Null Encryption (Disallowed by Policy)
- Triple-DES as used in IKE/IPSec (Disallowed by Policy)

These algorithms are used for older version of WEP in non-FIPS mode.

6 Critical Security Parameters

The following Critical Security Parameters (CSPs) are used by the module (unless explicitly specified, a CSP is applicable to all approved modes of operation):

Table 6.1 - Critical Security Parameters

#	Name	Algorithm/Key Size	Generation/Use	Storage	Zeroization
General Keys/CSPs					
1	Key Encryption Key (KEK) – Not considered a CSP	Triple-DES (192 bits)	Hardcoded during manufacturing. Used only to obfuscate keys stored in the flash, not for key transport. (3 Key, CBC)	Stored in Flash memory (plaintext)	The zeroization requirements do not apply to this key as it is not considered a CSP.
2	DRBG entropy input	SP 800-90a CTR_DRBG (512 bits)	Entropy inputs to DRBG function used to construct the DRBG seed. 64 bytes are gotten from the entropy source on each call by any service that requires a random number.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
3	DRBG seed	SP 800-90a CTR_DRBG (384-bits)	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
4	DRBG Key	SP 800-90a CTR_DRBG (256 bits)	This is the DRBG key used for SP 800-90a CTR_DRBG.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
5	DRBG V	SP 800-90a CTR_DRBG V (128 bits)	Internal V value used as part of SP 800-90a CTR_DRBG.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

6	Diffie-Hellman private key	Diffie-Hellman Group 14 (224 bits)	Generated internally by calling FIPS approved DRBG (Certs. #528, #1188) to derive Diffie-Hellman shared secret used in both IKEv1 and IKEv2.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
7	Diffie-Hellman public key	Diffie-Hellman Group 14 (2048 bits)	Derived internally in compliance with Diffie-Hellman key agreement scheme. Used for establishing DH shared secret.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
8	Diffie-Hellman shared secret	Diffie-Hellman Group 14 (2048 bits)	Established during Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
9	EC Diffie-Hellman private key	EC Diffie-Hellman (Curves: P-256 or P-384).	Generated internally by calling FIPS approved DRBG (Certs. #528, #1188) during EC Diffie-Hellman Exchange. Used for establishing ECDH shared secret.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
10	EC Diffie-Hellman public key	EC Diffie-Hellman (Curves: P-256 or P-384).	Derived internally in compliance with EC Diffie-Hellman key agreement scheme. Used for establishing ECDH shared secret.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
11	EC Diffie-Hellman shared secret	EC Diffie-Hellman (Curves: P-256 or P-384)	Established during EC Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
12	Factory CA Public Key	RSA (2048 bits)	This is RSA public key. Loaded into the module during manufacturing. Used for Firmware verification.	Stored in TPM.	As this is a public key, the zeroization requirements do not apply

IPSec/IKE[10]					
13	IKEv1 Pre-shared secret[11]	Shared secret (8 - 64 ASCII or 64 HEX characters)	Entered by CO role. Used for IKEv1 peers authentication.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash' or by overwriting with a new secret
14	skeyid	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv1 peers. It was established via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving other keys in IKEv1 protocol implementation.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module.
15	skeyid_d	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv1 peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving IKEv1 session authentication key.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
16	SKEYSEED	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv2 peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving other keys in IKEv2 protocol.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
17	IKE session authentication key	HMAC-SHA-1/256/384 (160/256/384 bits)	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IKEv1/IKEv2 payload integrity	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

[10] Not used in Mesh Point modes of operation

[11] Applicable only to Remote AP and Mesh Portal modes

			verification.		
18	IKE session encryption key	AES (128/192/256 bits, CBC)	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IKE payload protection.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
19	IPSec session encryption keys	AES (CBC) and AES-GCM (128/192/256 bits)	The IPsec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IPSec traffics protection. The IPsec session encryption keys can also be used for the Double Encrypt feature.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
20	IPSec session authentication keys	HMAC-SHA-1 (160 bits)	The IPsec (IKE Phase II) authentication key. This key is derived via using the KDF defined in SP800-135 KDF (IKEv1/IKEv2). Used for IPSec traffics integrity verification.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
21	IKE RSA Private Key	RSA private key (2048 bits)	This is the RSA private key. This key is generated by the module in compliance with FIPS 186-4 RSA key pair generation method. In both IKEv1 and IKEv2, DRBG (Certs. #528, #1188) is called for key generation. It is used for RSA signature signing in either IKEv1 or IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK	Zeroized by using command ‘ap wipe out flash’

22	IKE RSA public key	RSA public key (2048 bits)	This is the RSA public key. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module. It is used for RSA signature verification in either IKEv1 or IKEv2. This key can also be entered by the CO.	Stored in Flash memory in plaintext	Zeroized by using command 'ap wipe out flash'
23	IKE ECDSA Private Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA private key. This key is generated by the module in compliance with FIPS 186-4 ECDSA key pair generation method. In IKEv2, DRBG (Certs. #528, #1188) is called for key generation. It is used for ECDSA signature signing in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash'.
24	IKE ECDSA Public Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA public key. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module. It is used for ECDSA signature verification in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash'
802.11i[12]					
25	802.11i Pre-shared secret	Shared secret (8-63 ASCII characters, or 64 HEX characters)	Entered by CO role. Used for 802.11i client/server authentication.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash' or by overwriting with a new secret.

[12] While operating in Mesh Point or Mesh Portal mode, the AP will only use PSK for 802.11. RAP and CPsec modes use both Certificate-based and PSK-based 802.11

26	802.11i Pair-Wise Master key (PMK)	Shared secret (256 bits)	The PMK is transported to the module, protected by IPSec secure tunnel. Used to derive the Pairwise Transient Key (PTK) for 802.11i communications.	Stored in SDRAM (plaintext)	Zeroized by rebooting the module
27	802.11i Pairwise Transient Key (PTK)	384 bit HMAC	This key is used to derive 802.11i session key by using the KDF defined in SP800-108.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
28	802.11i session key	AES-CCM (128 bits)	Derived during 802.11i 4-way handshake by using the KDF defined in SP800-108 then used as the session key.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
29	802.11i Group Master Key (GMK)	Shared secret (256 bits)	Generated by calling DRBG (Certs. #528, #1188). Used to derive 802.11i Group Transient Key GTK.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
30	802.11i Group Transient Key (GTK)	AES-CCM (256 bits)	Derived from 802.11 GMK by using the KDF defined in SP800-108. The GTK is the 802.11i session key used for broadcast communications protection.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

Please note that:

- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 1. FIPS approved DRBG (Certs. #528, #1188) is used for IV generation and 96 bits of IV is supported.
- For keys identified as being “Generated internally by calling FIPS approved DRBG", the generated seed used in the asymmetric key generation is an unmodified output from the DRBG.
- The module generates a minimum of 256 bits of entropy for use in key generation.
- In Remote AP FIPS mode, all CSPs are applicable.
- In CPSec Protected AP FIPS mode, the IKEv1 PSK CSPs are not applicable.
- In Mesh Point FIPS modes, all IPSec/IKE CSPs are not applicable.
- CSPs labeled as “Entered by CO” are transferred into the module from the Mobility Controller via IPSec.

7 Self Tests

The module performs Power On Self-Tests regardless the modes (non-FIPS mode, Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode, Mesh Portal FIPS mode or Mesh Point FIPS mode). In addition, the module also performs Conditional tests after being configured into either Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode, Mesh Portal FIPS mode or Mesh Point FIPS mode. In the event any self-test fails, the module enters an error state, logs the error, and reboots automatically.

The module performs the following power on self-tests:

ArubaOS OpenSSL Module:

- SHA (SHA-1, SHA-256, SHA-384, SHA-512) KATs
- HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) KATs
- Triple-DES (encrypt/decrypt) KATs
- AES (Encrypt/Decrypt) KATs
- ECDSA (Sign/Verify) KATs
- RSA (Sign/Verify) KATs
- DSA (Sign/Verify) KATs
- DRBG KATs
- ECDH (P-256) KAT
- DH (2048) KAT
- KDF108 KAT

ArubaOS Crypto Module

- SHA (SHA-1, SHA-256, SHA-384, SHA-512) KATs
- HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) KATs
- AES (Encrypt/Decrypt) KATs
- AES-GCM (Encrypt/Decrypt) KATs
- Triple-DES (Encrypt/Decrypt KATs)
- ECDSA (Sign/Verify) KATs
- RSA (Sign/Verify) KATs
- DSA (Sign/Verify) KATs
- ECDH (P-256, P-384) Pairwise Consistency Tests
- DH (2048) Pairwise Consistency Tests

ArubaOS UBOOT Bootloader Module

- Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256 (the integrity test is the KAT)

Aruba AP Hardware algorithm implementation power on self-tests:

- AES (encrypt/decrypt) KATs
- AES-CCM (encrypt/decrypt) KATs
- AES-GCM (encrypt/decrypt) KATs
- Triple-DES (encrypt/decrypt) KATs
- SHA-1KAT
- HMAC (HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512) KATs

The following Conditional Self-tests are performed in the AP.

ArubaOS OpenSSL Module

- CRNG Test to Approved DRBG
- SP800-90A Section 11.3 Health Tests for DRBG (Instantiate, Generate and Reseed).
- ECDSA Pairwise Consistency Test
- RSA Pairwise Consistency Test
- CRNG Test to NDRNG

ArubaOS Crypto Module

- RSA Pairwise Consistency Test
- ECDSA Pairwise Consistency Test

ArubaOS UBOOT Bootloader Module

- Firmware Load Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256

These self-tests are run for the hardware cryptographic implementation as well as for the Aruba OpenSSL and ArubaOS cryptographic module implementations.

In the event of a KATs failure, the AP logs different messages, depending on the error.

For an ArubaOS OpenSSL AP module and ArubaOS cryptographic module KAT failure:

```
AP rebooted [DATE][TIME] : Restarting System, SW FIPS KAT failed
```

For an AES Atheros hardware POST failure:

```
Starting HW SHA1 KAT ...Completed HW SHA1 AT
Starting HW HMAC-SHA1 KAT ...Completed HW HMAC-SHA1 KAT
Starting HW AES KAT ...Restarting system.
```

8 Secure Operation

The module can be configured to be in the following FIPS approved modes of operations via corresponding Aruba Mobility Controllers that have been certified to FIPS level 2:

- Remote AP FIPS mode – When the module is configured as a Remote AP, it is intended to be deployed in a remote location (relative to the Mobility Controller). The module provides cryptographic processing in the form of IPSec for all traffic to and from the Mobility Controller.
- Control Plane Security (CPSec) Protected AP FIPS mode – When the module is configured as a Control Plane Security protected AP it is intended to be deployed in a local/private location (LAN, WAN, MPLS) relative to the Mobility Controller. The module provides cryptographic processing in the form of IPSec for all Control traffic to and from the Mobility Controller.
- Mesh Portal FIPS mode – When the module is configured in Mesh Portal mode, it is intended to be connected over a physical wire to the mobility controller. These modules serve as the connection point between the Mesh Point and the Mobility Controller. Mesh Portals communicate with the Mobility Controller through IPSec and with Mesh Points via 802.11i session. The Crypto Officer role is the Mobility Controller that authenticates via IKEv1/IKEv2 pre-shared key or RSA/ECDSA certificate authentication method, and Users are the "n" Mesh Points that authenticate via 802.11i preshared key.
- Mesh Point FIPS mode – an AP that establishes all wireless path to the Mesh portal in FIPS mode over 802.11 and an IPSec tunnel via the Mesh Portal to the controller.

In addition, the module also supports a non-FIPS mode – an un-provisioned AP, which by default does not serve any wireless clients. The Crypto Officer must first enable and then provision the AP into a FIPS AP mode of operation. Only firmware updates signed with SHA-256/RSA 2048 are permitted. The user is responsible for zeroizing all CSPs when switching modes.

The instructions for provisioning the APs are in the User Guide which is provided in Section 8.2 below. An important point in the Aruba APs is that to change configurations from any one mode to any other mode requires the module to be re-provisioned and rebooted before any new configured mode can be enabled.

The access point is managed by an Aruba Mobility Controller in FIPS mode, and access to the Mobility Controller's administrative interface via a non-networked general purpose computer is required to assist in placing the module in FIPS mode. The controller used to provision the AP is referred to as the "staging controller". The staging controller must be provisioned with the appropriate firmware image for the module, which has been validated to FIPS 140-2, prior to initiating AP provisioning. Additionally, if a Mobility Master Appliance is deployed in the environment, provisioning of the APs can be performed by passing policies down from the Mobility Master to the Mobility Controller which then provisions the AP. The Crypto Officer shall perform the following steps to ensure the APs are placed in the secure operational state:

1. Apply TELs according to the directions in section 3.2.
2. Enable FIPS mode on the staging controller: Log into the staging controller via SSH and enter the following commands: "configure terminal", "fips enable", "write memory", "reload" "y".
3. Connect the module via an Ethernet cable to the staging controller; note that this should be a direct connection, with no intervening network or devices; if PoE is being supplied by an injector, this represents the only exception. That is, nothing other than a PoE injector should be present between the module and the staging controller.
4. Provision the AP into one of the 4 modes listed above, as indicated in the ArubaOS User Guide (see section 8.2 for link).
5. Via the logging facility of the staging controller, ensure that the module (the AP) is successfully provisioned with firmware and configuration.

6. Terminate the administrative session.
7. Disconnect the module from the staging controller, and install it on the deployment network; when power is applied, the module will attempt to discover and connect to an Aruba Mobility Controller on the network

Once the AP has been provisioned, it is considered to be in FIPS mode provided that the guidelines on services, algorithms, physical security and key management found in this Security Policy are followed.

8.1 Verifying the FIPS mode

When connecting the AP to the controller for initial configuration, the Mobility Controller will provide the AP with a FIPS firmware image for use. While running this image, the AP will be compliant with FIPS requirements provided that the guidelines on services, algorithms, physical security and key management found in this Security Policy are followed. To verify that the image is being run, the CO can enter 'show ap image' on the controller to verify the correct image is present on the device. Additionally, the CO can enter 'fips enable' if connecting to a non-FIPS enabled Controller to ensure the Access Point only accepts FIPS approved cryptography.

8.2 Full Documentation

Can be found at:

https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=34189

8.3 Disallowed FIPS Mode Configurations

When you enable FIPS mode, the following configuration options are forcibly disallowed:

- All WEP features
- WPA
- TKIP mixed mode
- Any combination of DES, MD5, and PPTP

When you enable FIPS mode, the following configuration options are disallowed by policy:

- USB CSR-Key Storage
- Telnet
- Firmware images signed with SHA- 1
- Enhanced PAPI Security
- Null Encryption
- EAP-TLS Termination
- IPSec/IKE using Triple-DES